University Anonymizable Public-Key Encryption(New Trends in Theory of Computation and Algorithm)

AUTHOR(S):

Hayashi, Ryotaro; Tanaka, Keisuke

数理解析研究所講究録
1489 巻 2006 年 36-42

一般的に匿名化可能な暗号方式
Universally Anonymizable Public-Key Encryption

林 良太郎* 田中 圭介*
Ryotaro Hayashi Keisuke Tanaka

東京工業大学 数理・計算科学専攻
Dept. of Mathematical and Computing Sciences, Tokyo Institute of Technology

Abstract— We first propose the notion of universally anonymizable public-key encryption. Suppose that we have the encrypted data made with the same security parameter, and that these data do not satisfy the anonymity property. Consider the situation that we would like to transform these encrypted data to those with the anonymity property without decrypting these encrypted data. In this paper, in order to formalize this situation, we propose a new property for public-key encryption called universal anonymizability. If we use a universally anonymizable public-key encryption scheme, not only the person who made the ciphertexts, but also anyone can anonymize the encrypted data without using the corresponding secret key. We then propose universally anonymizable public-key encryption schemes based on the ElGamal encryption scheme, the Cramer-Shoup encryption scheme, and RSA-OAEP, and prove their security.

Keywords: encryption, anonymity, key-privacy, ElGamal, Cramer-Shoup, RSA-OAEP

1 Introduction

The classical security requirement of public-key encryption schemes is that it provides privacy of the encrypted data. Popular formalizations such as indistinguishability or non-malleability, under either the chosen-plaintext or the chosen-ciphertext attacks are directed at capturing various data-privacy requirements.

Bellare, Boldyreva, Desai, and Pointcheval [1] proposed a new security requirement of encryption schemes called "key-privacy" or "anonymity." It asks that an encryption scheme provides (in addition to privacy of the data being encrypted) privacy of the key under which the encryption was performed. That is, if an encryption scheme provides the key-privacy, then the receiver is anonymous from the point of view of the adversary.

In addition to the notion of key-privacy, they provided the RSA-based anonymous public-key encryption scheme, RSA-RAEP, which is a variant of RSA-OAEP (Bellare and Rogaway [2], Fujisaki, Okamoto, Pointcheval, and Stern [6]). Recently, Hayashi, Okamoto, and Tanaka [8] proposed the RSA-based anonymous encryption scheme by using the RSACD function. Hayashi and Tanaka [9] constructed the RSA-based anonymous encryption scheme by using the sampling twice technique. In [9], they also mentioned the scheme with the expanding technique for comparison, however, there is no security proof.

With respect to the discrete-log based schemes, Bellare, Boldyreva, Desai, and Pointcheval [1] proved that the ElGamal and the Cramer-Shoup encryption schemes provide the anonymity property when all of the users use a common group.

In this paper, we consider the following situation. In order to send e-mails, all members of the company use the encryption scheme which does not provide the anonymity property. They consider that e-mails sent to the inside of the company do not have to be anonymized and it is sufficient to be encrypted the data. However, when e-mails are sent to the outside of the company, they want to anonymize them for preventing the eavesdropper on the public network.

A trivial answer for this problem is that all members use the encryption scheme with the anonymity property. However, generally speaking, we require some computational costs to create ciphertexts with the anonymity property. In fact, the RSA-based anonymous encryption schemes proposed in [1, 8, 9], which are based on RSA-OAEP, are not efficient with respect to the encryption cost or the size of ciphertexts, compared with RSA-OAEP (See Figure 1. Here, k, k_0, k_1 are security parameters and we assume that N is uniformly dis-

* Supported in part by NTT Information Sharing Platform Laboratories and Grant-in-Aid for Scientific Research, Ministry of Education, Culture, Sports, Science, and Technology, 16092206.

	RSA-OAEP	Sampling Twice [9]	RSA-RAEP [1]	RSACD [8]	Expanding
anonymity	No	Yes	Yes	Yes	Yes
# of mod. exp. to encrypt (average / worst)	1 / 1	2 / 2	1.5 / k_1	1.5 / 2	1 / 1
# of random bits to encrypt (average / worst)	k_0	$2k_0+k+3$ / $2k_0+k+3$	$1.5k_0$ / k_1k_0	$1.5k_0$ / $1.5k_0$	k_0+160 / k_0+160
size of ciphertexts	k	k	k	k	$k+160$

Figure 1: The costs of the encryption schemes.

tributed in $(2^{k-1}, 2^k)$.). Since the members do not require to anonymize the e-mails, it would be better to use the standard encryption scheme within the company.

We propose another way to solve this. Consider the situation that not only the person who made the ciphertexts, but also anyone can transform the encrypted data to those with the anonymity property without decrypting these encrypted data. If we have this situation, we can make an e-mail gateway which can transform encrypted e-mails to those with the anonymity property without using the corresponding secret key when they are sent to the outside of the company.

Furthermore, we can use this e-mail gateway in order to guarantee the anonymity property for e-mails sent to the outside of the company. The president of the company may consider that all e-mails sent to the outside of the company should be anonymized. In this case, even if someone tries to send e-mails to the outside of the company without anonymization, the e-mails passing through the e-mail gateway are always anonymized.

In this paper, in order to formalize this idea, we propose a special type of public-key encryption scheme called a *universally anonymizable public-key encryption scheme*. A universally anonymizable public-key encryption scheme consists of a standard public-key encryption scheme $\mathcal{PE}$ and two additional algorithms, that is, an anonymizing algorithm $\mathcal{UA}$ and a decryption algorithm $\mathcal{DA}$ for anonymized ciphertexts. We can use $\mathcal{PE}$ as a standard encryption scheme which is not necessary to have the anonymity property. Furthermore, in this scheme, by using the anonymizing algorithm $\mathcal{UA}$, anyone who has a standard ciphertext can anonymize it with its public key whenever she wants to do that. The receiver can decrypt the anonymized ciphertext by using the decryption algorithm $\mathcal{DA}$ for anonymized ciphertexts. Then, the adversary cannot know under which key the anonymized ciphertext was created.

To formalize the security properties for universally anonymizable public-key encryption, we define three requirements, the data-privacy on standard ciphertexts, that on anonymized ciphertexts, and the key-privacy.

We then propose the universally anonymizable public-key encryption schemes based on the ElGamal encryption scheme, the Cramer-Shoup encryption scheme, and RSA-OAEP, and prove their security.

We show the key-privacy property of our schemes by applying an argument in [1] with modification. The argument in [1] for the discrete-log based scheme depends heavily on the situation where all of the users employ a common group. However, in our discrete-log based schemes, we do not use the common group for obtaining the key-privacy property. Therefore, we cannot straightforwardly apply their argument to our schemes. To prove the key-privacy property of our schemes, we employ the idea described in [4] by Cramer and Shoup, where we encode the elements of QR_p (a group of quadratic residues modulo p) where $p = 2q + 1$ and p, q are prime to those of $\mathbf{Z}_q$. This encoding plays an important role in our schemes. We also employ the expanding technique. With this technique, if we get the ciphertext, we expand it to the common domain. This technique was proposed by Desmedt [5]. In [7], Galbraith and Mao used this technique for the undeniable signature scheme. In [11], Rivest, Shamir, and Tauman also used this technique for the ring signature scheme.

The organization of this paper is as follows. In Section 2, we formulate the notion of universally anonymizable public-key encryption and its security properties. We propose the universally anonymizable public-key encryption scheme based on the ElGamal encryption scheme in Section 3, that based on the Cramer-Shoup encryption scheme in Section 4, and that based on RSA-OAEP in Section 5.

Due to lack of space, details have been omitted from this paper. See the full version [10].

2 Universally Anonymizable Public-Key Encryption

In this section, we propose the definition of universally anonymizable public-key encryption schemes and its security properties.

2.1 The Definition

We formalize the notion of universally anonymizable public-key encryption schemes as follows.

Definition 1. *A universally anonymizable public-key encryption scheme* $\mathcal{UAPE} = ((\mathcal{K}, \mathcal{E}, \mathcal{D}), \mathcal{UA}, \mathcal{DA})$ *consists of a public-key encryption scheme* $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ *and two other algorithms.*

- *The key generation algorithm* $\mathcal{K}$ *is a randomized algorithm that takes as input a security parameter* k *and returns a pair* (pk, sk) *of keys, a public key and a matching secret key.*
- *The encryption algorithm* $\mathcal{E}$ *is a randomized algorithm that takes the public key* pk *and a plaintext* m *and returns a standard ciphertext* c*.*
- *The decryption algorithm* $\mathcal{D}$ *for standard ciphertexts is a deterministic algorithm that takes the secret key* sk *and a standard ciphertext* c *and returns the corresponding plaintext* m *or a special symbol* $\perp$ *to indicate that the standard ciphertext is invalid.*
- *The anonymizing algorithm* $\mathcal{UA}$ *is a randomized algorithm that takes the public key* pk *and a standard ciphertext* c *and returns an anonymized ciphertext* c'*.*
- *The decryption algorithm* $\mathcal{DA}$ *for anonymized ciphertexts is a deterministic algorithm that takes the secret key* sk *and an anonymized ciphertext* c' *and returns the corresponding plaintext* m *or a special symbol* $\perp$ *to indicate that the anonymized ciphertext is invalid.*

We require the standard correctness condition. That is, for any (pk, sk) *outputted by* $\mathcal{K}$ *and* $m \in \mathcal{M}(pk)$ *where* $\mathcal{M}(pk)$ *denotes the message space of* pk*,* $m = \mathcal{D}_{sk}(\mathcal{E}_{pk}(m))$ *and* $m = \mathcal{DA}_{sk}(\mathcal{UA}_{pk}(\mathcal{E}_{pk}(m)))$*.*

In the universally anonymizable public-key encryption scheme, we can use $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ as a standard encryption scheme. Furthermore, in this scheme, by using the anonymizing algorithm $\mathcal{UA}$, anyone who has a standard ciphertext can anonymize it whenever she wants to do that. The receiver can decrypt the anonymized ciphertext by using the decryption algorithm $\mathcal{DA}$ for anonymized ciphertexts.

2.2 Security Properties

We now define security properties with respect to universally anonymizable public-key encryption schemes.

2.2.1 Data-Privacy

We define the security property called *data-privacy* of universally anonymizable public-key encryption schemes. The definition is based on the indistinguishability for standard public-key encryption schemes.

We can consider two types of data-privacy, that is, the data-privacy on standard ciphertexts and that on anonymized ciphertexts. We first describe the definition of the data-privacy on standard ciphertexts.

Definition 2 (Data-Privacy on Standard Ciphertexts). *Let* $b \in \{0, 1\}$ *and* $k \in \mathbf{N}$*. Let* $A_{\mathrm{cpa}} = (A^1_{\mathrm{cpa}}, A^2_{\mathrm{cpa}})$*,* $A_{\mathrm{cca}} = (A^1_{\mathrm{cca}}, A^2_{\mathrm{cca}})$ *be adversaries that run in two stages and where* A_{cca} *has access to the oracles* $\mathcal{D}_{sk_0}(\cdot)$*,* $\mathcal{D}_{sk_1}(\cdot)$*,* $\mathcal{DA}_{sk_0}(\cdot)$*, and* $\mathcal{DA}_{sk_1}(\cdot)$*. Note that* si *is the state information. It contains* pk, m_0, m_1*, and so on. For* atk $\in$ {cpa, cca}*, we consider the following experiment:*

$$\begin{array}{l}\textbf{Experiment } \mathbf{Exp}^{\text{dataS-atk-}b}_{\mathcal{UAPE}, A_{\mathrm{atk}}}(k) \\ \quad (pk, sk) \leftarrow \mathcal{K}(k);\ (m_0, m_1, \mathrm{si}) \leftarrow A^1_{\mathrm{atk}}(pk) \\ \quad c \leftarrow \mathcal{E}_{pk}(m_b);\ d \leftarrow A^2_{\mathrm{atk}}(c, \mathrm{si});\ \textbf{return } d\end{array}$$

Note that $m_0, m_1 \in \mathcal{M}(pk)$*. Above it is mandated that* A^2_{cca} *never queries the challenge ciphertext* c *to either* $\mathcal{D}_{sk_0}(\cdot)$ *or* $\mathcal{D}_{sk_1}(\cdot)$*, and it is also mandated that* A^2_{cca} *never queries either the anonymized ciphertext* $\tilde{c} \in \{\mathcal{UA}_{pk_0}(c)\}$ *to* $\mathcal{DA}_{sk_0}(\cdot)$ *or* $\tilde{c} \in \{\mathcal{UA}_{pk_1}(c)\}$ *to* $\mathcal{DA}_{sk_1}(\cdot)$*. For* atk $\in$ {cpa, cca}*, we define the advantage via*

$$\mathbf{Adv}^{\text{dataS-atk}}_{\mathcal{UAPE}, A_{\mathrm{atk}}}(k) = |p_1^{\text{dataS-atk}} - p_0^{\text{dataS-atk}}|$$

where

$$p_i^{\text{dataS-atk}} = \Pr[\mathbf{Exp}^{\text{dataS-atk-}i}_{\mathcal{UAPE}, A_{\mathrm{atk}}}(k) = 1].$$

We say that the universally anonymizable public-key encryption scheme $\mathcal{UAPE}$ *provides the data-privacy on standard ciphertexts against the chosen plaintext attack (respectively the adaptive chosen ciphertext attack) if* $\mathbf{Adv}^{\text{dataS-cpa}}_{\mathcal{UAPE}, A_{\mathrm{cpa}}}(k)$ *(resp.* $\mathbf{Adv}^{\text{dataS-cca}}_{\mathcal{UAPE}, A_{\mathrm{cca}}}(k)$*) is negligible for any adversary* A *whose time complexity is polynomial in* k*.*

In the above experiment, if the challenge is c, then anyone can compute $\mathcal{UA}_{pk_0}(c)$. Therefore, in the CCA setting, we restrict the oracle access to $\mathcal{DA}$ as described above.

We next describe the definition of the data-privacy on anonymized ciphertexts.

Definition 3 (Data-Privacy on Anonymized Ciphertexts). *Let* $b \in \{0, 1\}$ *and* $k \in \mathbf{N}$*. Let* $A_{\mathrm{cpa}} = (A^1_{\mathrm{cpa}}, A^2_{\mathrm{cpa}})$*,* $A_{\mathrm{cca}} = (A^1_{\mathrm{cca}}, A^2_{\mathrm{cca}})$ *be adversaries*

that run in two stages and where A_{cca} has access to the oracles $\mathcal{D}_{sk_0}(\cdot)$, $\mathcal{D}_{sk_1}(\cdot)$, $\mathcal{DA}_{sk_0}(\cdot)$, and $\mathcal{DA}_{sk_1}(\cdot)$. For atk $\in$ {cpa, cca}*, we consider the following experiment:*

Experiment $\mathbf{Exp}^{\text{dataA-atk-}b}_{\mathcal{UAPE},A_{\mathrm{atk}}}(k)$
$(pk, sk) \leftarrow \mathcal{K}(k)$; $(m_0, m_1, \mathrm{si}) \leftarrow A^1_{\mathrm{atk}}(pk)$
$c \leftarrow \mathcal{E}_{pk}(m_b)$; $c' \leftarrow \mathcal{UA}_{pk}(c)$; $d \leftarrow A^2_{\mathrm{atk}}(c', \mathrm{si})$
return d

Note that $m_0, m_1 \in \mathcal{M}(pk)$. Above it is mandated that A^2_{cca} never queries the challenge c' to either $\mathcal{DA}_{sk_0}(\cdot)$ or $\mathcal{DA}_{sk_1}(\cdot)$. For atk $\in$ {cpa, cca}*, we define the advantage via*

$$\mathbf{Adv}^{\text{dataA-atk}}_{\mathcal{UAPE},A_{\mathrm{atk}}}(k) = |p_1^{\text{dataA-atk}} - p_0^{\text{dataA-atk}}|$$

where

$$p_i^{\text{dataA-atk}} = \Pr[\mathbf{Exp}^{\text{dataA-atk-}i}_{\mathcal{UAPE},A_{\mathrm{atk}}}(k) = 1].$$

We say that the universally anonymizable public-key encryption scheme $\mathcal{UAPE}$ provides the data-privacy on anonymized ciphertexts against the chosen plaintext attack (respectively the adaptive chosen ciphertext attack) if $\mathbf{Adv}^{\text{dataA-cpa}}_{\mathcal{UAPE},A_{\mathrm{cpa}}}(k)$ (resp. $\mathbf{Adv}^{\text{dataA-cca}}_{\mathcal{UAPE},A_{\mathrm{cca}}}(k)$) is negligible for any adversary A whose time complexity is polynomial in k.

Remark 1. *In the CPA setting, if there exists an algorithm which breaks the data-privacy on anonymized ciphertexts, then we can break that on standard ciphertexts by applying the anonymizing algorithm to the standard ciphertexts and passing the resulting anonymized ciphertexts to the adversary which breaks the data-privacy on anonymized ciphertexts. Therefore, in the CPA setting, it is sufficient that the universally anonymizable public-key encryption scheme provides the data-privacy of standard ciphertexts.*

On the other hand, in the CCA setting, the data privacy on standard ciphertexts does not always imply that on anonymized ciphertexts, since the oracle access of the adversary attacking the data privacy on standard ciphertexts is restricted more strictly than that on anonymized ciphertexts.

2.2.2 Key-Privacy

We define the security property called *key-privacy* of universally anonymizable public-key encryption schemes. If the scheme provides the key-privacy, the adversary cannot know under which key the anonymized ciphertext was created.

Definition 4 (Key-Privacy). *Let $b \in \{0, 1\}$ and $k \in \mathbf{N}$. Let $A_{\mathrm{cpa}} = (A^1_{\mathrm{cpa}}, A^2_{\mathrm{cpa}})$, $A_{\mathrm{cca}} = (A^1_{\mathrm{cca}}, A^2_{\mathrm{cca}})$ be adversaries that run in two stages and where A_{cca} has access to the oracles $\mathcal{D}_{sk_0}(\cdot)$, $\mathcal{D}_{sk_1}(\cdot)$, $\mathcal{DA}_{sk_0}(\cdot)$, and $\mathcal{DA}_{sk_1}(\cdot)$. For* atk $\in$ {cpa, cca}*, we consider the following experiment:*

Experiment $\mathbf{Exp}^{\text{key-atk-}b}_{\mathcal{UAPE},A_{\mathrm{atk}}}(k)$
$(pk_0, sk_0) \leftarrow \mathcal{K}(k)$; $(pk_1, sk_1) \leftarrow \mathcal{K}(k)$
$(m_0, m_1, \mathrm{si}) \leftarrow A^1_{\mathrm{atk}}(pk_0, pk_1)$; $c \leftarrow \mathcal{E}_{pk_b}(m_b)$
$c' \leftarrow \mathcal{UA}_{pk_b}(c)$; $d \leftarrow A^2_{\mathrm{atk}}(c', \mathrm{si})$; **return** d

Note that $m_0 \in \mathcal{M}(pk_0)$ and $m_1 \in \mathcal{M}(pk_1)$. Above it is mandated that A^2_{cca} never queries the challenge c' to either $\mathcal{DA}_{sk_0}(\cdot)$ or $\mathcal{DA}_{sk_1}(\cdot)$. For atk $\in$ {cpa, cca}*, we define the advantage via*

$$\mathbf{Adv}^{\text{key-atk}}_{\mathcal{UAPE},A_{\mathrm{atk}}}(k) = |p_1^{\text{key-atk}} - p_0^{\text{key-atk}}|$$

where

$$p_i^{\text{key-atk}} = \Pr[\mathbf{Exp}^{\text{key-atk-}i}_{\mathcal{UAPE},A_{\mathrm{atk}}}(k) = 1].$$

We say that the universally anonymizable public-key encryption scheme $\mathcal{UAPE}$ provides the key-privacy
against the chosen plaintext attack (resp. the adaptive chosen ciphertext attack) if $\mathbf{Adv}^{\text{key-cpa}}_{\mathcal{UAPE},A_{\mathrm{cpa}}}(k)$ (resp. $\mathbf{Adv}^{\text{key-cca}}_{\mathcal{UAPE},A_{\mathrm{cca}}}(k)$) is negligible for any adversary A whose time complexity is polynomial in k.

Bellare, Boldyreva, Desai, and Pointcheval [1] proposed a security requirement of public-key encryption schemes called "key-privacy." Similar to the above definition, it asks that the encryption provides privacy of the key under which the encryption was performed. In addition to the property of the universal anonymizability, there are two differences between their definition and ours.

In [1], they defined the encryption scheme with some *common-key* which contains the common parameter for all users to obtain the key-privacy property. For example, in the discrete-log based schemes such that the ElGamal and the Cramer-Shoup encryption schemes, the common key contains a common group G, and the encryption is performed over the common group for all uses.

On the other hand, in our definition, we do not prepare any common key for obtaining the key-privacy property. In the universally anonymizable public-key encryption scheme, we can use the standard encryption scheme which is not necessary to have the key-privacy property. In addition to it, anyone can anonymize the ciphertext by using its public key whenever she want to do that, and the adversary cannot know under which key the anonymized ciphertext was created.

The definition in [1], they considered the situation that the message space was common to each user. Therefore, in the experiment of their definition, the adversary chooses only one message m

from the common message space and receives a ciphertext of m encrypted with one of two keys pk_0 and pk_1.

In our definition, we do not use common parameter and the message spaces for users may be different even if the security parameter is fixed. In fact, in Sections 3 and 4, we propose the encryption schemes whose message spaces for users are different. Therefore, in the experiment of our definition, the adversary chooses two messages m_0 and m_1 where m_0 and m_1 are in the message spaces for pk_0 and pk_1, respectively, and receives either a ciphertext of m_0 encrypted with pk_0 or a ciphertext of m_1 encrypted with pk_1. The ability of the adversary with two messages m_0 and m_1 might be stronger than that with one message m.

We say that a universally anonymizable public-key encryption scheme $\mathcal{UAPE}$ is CPA-secure (resp. CCA-secure) if the scheme $\mathcal{UAPE}$ provides the data-privacy on standard ciphertexts, that on anonymized ciphertexts, and the key-privacy against the chosen plaintext attack (resp. the adaptive chosen ciphertext attack).

3 ElGamal and its Universal Anonymizability

In this section, we propose a universally anonymizable ElGamal encryption scheme.

3.1 The ElGamal Encryption Scheme

Definition 5 (ElGamal). *The ElGamal encryption scheme $\mathcal{PE}^{\mathsf{EG}} = (\mathcal{K}^{\mathsf{EG}}, \mathcal{E}^{\mathsf{EG}}, \mathcal{D}^{\mathsf{EG}})$ is as follows. Note that $\mathcal{Q}$ is a QR-group generator with a safe prime which takes as input a security parameter k and returns (q, g) where q is k-bit prime, $p = 2q + 1$ is prime, and g is a generator of a cyclic group QR_p (a group of quadratic residues modulo p) of order q.*

Algorithm $\mathcal{K}^{\mathsf{EG}}(k)$

$(q, g) \leftarrow \mathcal{Q}(k)$; $x \xleftarrow{R} \mathbf{Z}_q$; $y \leftarrow g^x$

return $pk = (q, g, y)$ and $sk = (q, g, x)$

Algorithm $\mathcal{E}^{\mathsf{EG}}_{pk}(m)$

$r \xleftarrow{R} \mathbf{Z}_q$; $c_1 \leftarrow g^r$; $c_2 \leftarrow m \cdot y^r$; **return** (c_1, c_2)

Algorithm $\mathcal{D}^{\mathsf{EG}}_{sk}(c_1, c_2)$

$m \leftarrow c_2 \cdot c_1^{-x}$; **return** m

3.2 Universal Anonymizability of the ElGamal Encryption Scheme

We now consider the situation that there exists no common key, and in the above definition of the ElGamal encryption scheme, each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q + 1$ is also prime, and uses a group of quadratic residues modulo p. Therefore, each user U_i uses a different groups G_i for her encryption scheme and if she publishes the ciphertext directly (without anonymization) then the scheme does not provide the key-privacy. In fact, the adversary simply checks whether the ciphertext y is in the group G_i, and if $y \notin G_i$ then y was not encrypted by U_i. To anonymize the standard ciphertext of the ElGamal encryption scheme, we consider the following strategy in the anonymizing algorithm: (1) Compute a ciphertext c over each user's prime-order group. (2) Encode c to an element $\bar{c} \in \mathbf{Z}_q$ (the encoding function). (3) Expand $\bar{c}$ to the common domain (the expanding technique).

We describe the encoding function and the expanding technique.

3.2.1 The Encoding Function

Let p be safe prime (i.e. $q = (p-1)/2$ is also prime) and $QR_p \subset \mathbf{Z}_p^*$ a group of quadratic residues modulo p. Then we have $|QR_p| = q$ and

$$QR_p = \{1^2 \bmod p,\ 2^2 \bmod p, \cdots,\ q^2 \bmod p\}.$$

It is easy to see that QR_p is a cyclic group of order q, and each $g \in QR_p \backslash \{1\}$ is a generator of QR_p.

We now define a function $F_q : QR_p \to \mathbf{Z}_q$ as

$$F_q(x) = \min\left\{\pm x^{\frac{p-1}{4}} \bmod p\right\}.$$

Noticing that $\pm x^{\frac{p-1}{4}} \bmod p$ are the square roots of x modulo p, the function F_q is bijective and we have $F_q^{-1}(y) = y^2 \bmod p$. We call the function F_q an *encoding function*. We also define a *t-encoding function* $\bar{F}_{q,t} : (QR_p)^t \to (\mathbf{Z}_q)^t$. $\bar{F}_{q,t}$ takes as input $(x_1, \cdots, x_t) \in (QR_p)^t$ and returns $(y_1, \cdots, y_t) \in (\mathbf{Z}_q)^t$ where $y_i = F_q(x_i)$ for each $i \in \{1, \cdots, t\}$. It is easy to see that $\bar{F}_{q,t}$ is bijective and we can define $\bar{F}_{q,t}^{-1}$.

3.2.2 The Expanding Technique

In the expanding technique, we expand $\bar{c} \in \mathbf{Z}_q$ to the common domain $\{0,1\}^{k+k_b}$. In particular, we choose $t \xleftarrow{R} \{0, 1, 2, \cdots, \lfloor (2^{k+k_b} - \bar{c})/q \rfloor\}$ and set $c' \leftarrow \bar{c} + tq$.

Then, for any q where $|q| = k$, if $\bar{c}$ is uniformly chosen from $\mathbf{Z}_q$, then the statistical distance between the distribution of the output c' by the expanding technique and the uniform distribution over $\{0,1\}^{k+k_b}$ is less than $1/2^{k_b - 1}$. In the following, we define a set $\mathrm{M}_q^{k+k_b}[\bar{c}]$ as

$$\mathrm{M}_q^{k+k_b}[\bar{c}] = \{0, 1, 2, \ldots, \lfloor (2^{k+k_b} - \bar{c})/q \rfloor\}$$

and set $k_b = 160$.

3.2.3 Our Scheme

We now propose our universally anonymizable ElGamal encryption scheme. Our scheme provides the key-privacy against the chosen plaintext attack even if each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q + 1$ is also prime, and uses a group of quadratic residues modulo p.

Definition 6. *Our universally anonymizable ElGamal encryption scheme* $\mathcal{UAPE}^{\mathsf{EG}} = ((\mathcal{K}^{\mathsf{EG}}, \mathcal{E}^{\mathsf{EG}}, \mathcal{D}^{\mathsf{EG}}), \mathcal{UA}^{\mathsf{EG}}, \mathcal{DA}^{\mathsf{EG}})$ *consists of the ElGamal encryption scheme* $\mathcal{PE}^{\mathsf{EG}} = (\mathcal{K}^{\mathsf{EG}}, \mathcal{E}^{\mathsf{EG}}, \mathcal{D}^{\mathsf{EG}})$ *and two algorithms described as follows.*

Algorithm $\mathcal{UA}^{\mathsf{EG}}_{pk}(m)$
$(\bar{c}_1, \bar{c}_2) \leftarrow \bar{F}_{q,2}(c_1, c_2)$
$t_1 \xleftarrow{R} \mathrm{M}_q^{k+160}[\bar{c}_1]$; $t_2 \xleftarrow{R} \mathrm{M}_q^{k+160}[\bar{c}_2]$
$c_1' \leftarrow \bar{c}_1 + t_1 q$; $c_2' \leftarrow \bar{c}_2 + t_2 q$
return (c_1', c_2')

Algorithm $\mathcal{DA}^{\mathsf{EG}}_{sk}(c_1', c_2')$
$\bar{c}_1 \leftarrow c_1' \bmod q$; $\bar{c}_2 \leftarrow c_2' \bmod q$
$(c_1, c_2) \leftarrow \bar{F}^{-1}_{q,2}(\bar{c}_1, \bar{c}_2)$; $m \leftarrow \mathcal{D}^{\mathsf{EG}}_{sk}(c_1, c_2)$
return m

Our universally anonymizable ElGamal encryption scheme is CPA-secure assuming that the DDH problem for $\mathcal{Q}$ is hard. (The proof is available in the full version [10].)

4 Cramer-Shoup and its Universal Anonymizability

In this section, we propose a universally anonymizable Cramer-Shoup encryption scheme.

4.1 The Cramer-Shoup Encryption Scheme

Before describing the Cramer-Shoup encryption scheme, we review the definition of families of hash functions.

Definition 7 (Families of Hash Functions). *A family of hash functions* $\mathcal{H} = (\mathcal{GH}, \mathcal{EH})$ *is defined by two algorithms. A probabilistic generator algorithm* $\mathcal{GH}$ *takes the security parameter* k *as input and returns a key* K*. A deterministic evaluation algorithm* $\mathcal{EH}$ *takes the key* K *and a string* $M \in \{0,1\}^*$ *and returns a string* $\mathcal{EH}_K(M) \in \{0,1\}^{k-1}$.

We now describe the Cramer-Shoup encryption scheme.

Definition 8 (Cramer-Shoup). *The Cramer-Shoup encryption scheme* $\mathcal{PE}^{\mathsf{CS}} = (\mathcal{K}^{\mathsf{CS}}, \mathcal{E}^{\mathsf{CS}}, \mathcal{D}^{\mathsf{CS}})$ *is defined as follows. Let* $\mathcal{H} = (\mathcal{GH}, \mathcal{EH})$ *be a family of hash functions. Note that* $\mathcal{Q}$ *is a QR-group generator with a safe prime.*

Algorithm $\mathcal{K}^{\mathsf{CS}}(k)$
$(q, g_1) \leftarrow \bar{\mathcal{G}}(k)$; $g_2 \xleftarrow{R} G_q$; $K \leftarrow \mathcal{GH}(k)$
$x_1, x_2, y_1, y_2, z \xleftarrow{R} \mathbb{Z}_q$
$c \leftarrow g_1^{x_1} g_2^{x_2}$; $d \leftarrow g_1^{y_1} g_2^{y_2}$; $h \leftarrow g_1^z$
return $pk = (g_1, g_2, c, d, h, K)$ and
$sk = (x_1, x_2, y_1, y_2, z)$

Algorithm $\mathcal{E}^{\mathsf{CS}}_{pk}(M)$
$r \xleftarrow{R} \mathbb{Z}_q$; $u_1 \leftarrow g_1^r$; $u_2 \leftarrow g_2^r$; $e \leftarrow h^r M$
$\alpha \leftarrow \mathcal{EH}_K(u_1, u_2, e)$; $v \leftarrow c^r d^{r\alpha}$
return (u_1, u_2, e, v)

Algorithm $\mathcal{D}^{\mathsf{CS}}_{sk}(u_1, u_2, e, v)$
$\alpha \leftarrow \mathcal{EH}_K(u_1, u_2, e)$
if $(u_1^{x_1 + y_1\alpha} u_2^{x_2 + y_2\alpha} = v)$ $M \leftarrow e/u_1^z$
else $M \leftarrow \perp$
return M

4.2 Universal Anonymizability of the Cramer-Shoup Encryption Scheme

We propose our universally anonymizable Cramer-Shoup encryption scheme. Our scheme provides the key-privacy against the adaptive chosen ciphertext attack even if each user chooses an arbitrary prime q where $|q| = k$ and $p = 2q + 1$ is also prime, and uses a group of quadratic residues modulo p.

Note that in our scheme we employ the encoding function and the expanding technique appeared in Section 3.

Definition 9. *Our universally anonymizable Cramer-Shoup encryption scheme* $\mathcal{UAPE}^{\mathsf{CS}} = ((\mathcal{K}^{\mathsf{CS}}, \mathcal{E}^{\mathsf{CS}}, \mathcal{D}^{\mathsf{CS}}), \mathcal{UA}^{\mathsf{CS}}, \mathcal{DA}^{\mathsf{CS}})$ *consists of the Cramer-Shoup encryption scheme* $\mathcal{PE}^{\mathsf{CS}} = (\mathcal{K}^{\mathsf{CS}}, \mathcal{E}^{\mathsf{CS}}, \mathcal{D}^{\mathsf{CS}})$ *and two algorithms described as follows.*

Algorithm $\mathcal{UA}^{\mathsf{CS}}_{pk}(m)$
$(\bar{u}_1, \bar{u}_2, \bar{e}, \bar{v}) \leftarrow \bar{F}_{q,4}(u_1, u_2, e, v)$
$t_1 \xleftarrow{R} \mathrm{M}_q^{k+160}(\bar{u}_1)$; $t_2 \xleftarrow{R} \mathrm{M}_q^{k+160}(\bar{u}_2)$
$t_3 \xleftarrow{R} \mathrm{M}_q^{k+160}(\bar{e})$; $t_4 \xleftarrow{R} \mathrm{M}_q^{k+160}(\bar{v})$
$c_1' \leftarrow \bar{c}_1 + t_1 q$; $c_2' \leftarrow \bar{c}_2 + t_2 q$
$e' \leftarrow \bar{e} + t_3 q$; $v' \leftarrow \bar{v} + t_4 q$
return (u_1', u_2', e', v')

Algorithm $\mathcal{DA}^{\mathsf{CS}}_{sk}(u_1', u_2', e', v')$
$\bar{u}_1 \leftarrow u_1' \bmod q$; $\bar{u}_2 \leftarrow u_2' \bmod q$
$\bar{e} \leftarrow e' \bmod q$; $\bar{v} \leftarrow v' \bmod q$
$(u_1, u_2, e, v) \leftarrow \bar{F}^{-1}_{q,4}(\bar{u}_1, \bar{u}_2, \bar{e}, \bar{v})$
$m \leftarrow \mathcal{D}^{\mathsf{CS}}_{sk}(u_1, u_2, e, v)$; **return** m

---

Our universally anonymizable Cramer-Shoup encryption scheme is CCA-secure assuming that the DDH problem for $\mathcal{Q}$ is hard and $\mathcal{H}$ is universal one-way. (The proof is available in the full version [10].)

5 RSA-OAEP and its Universal Anonymizability

In this section, we propose a universally anonymizable RSA-OAEP scheme.

5.1 RSA-OAEP

Definition 10 (RSA-OAEP). *RSA-OAEP* $\mathcal{PE}^{\mathsf{RO}} = (\mathcal{K}^{\mathsf{RO}}, \mathcal{E}^{\mathsf{RO}}, \mathcal{D}^{\mathsf{RO}})$ *is as follows. Let* k, k_0 *and* k_1 *be security parameters such that* $k_0+k_1 < k$. *This defines an associated plaintext-length* $n = k-k_0-k_1$. *The key generation algorithm* $\mathcal{K}^{\mathsf{RO}}$ *takes as input a security parameter* k *and runs the key generation algorithm of* RSA *to get* N, e, d. *It outputs the public key* $pk = (N, e)$ *and the secret key* $sk = d$. *The other algorithms are depicted below. Let* $G : \{0,1\}^{k_0} \to \{0,1\}^{n+k_1}$ *and* $H : \{0,1\}^{n+k_1} \to \{0,1\}^{k_0}$ *be hash functions. Note that* $[x]^{\ell}$ *denotes the* ℓ *most significant bits of* x, *and* $[x]_{\ell'}$ *denotes the* ℓ' *least significant bits of* x.

Algorithm $\mathcal{E}^{\mathsf{RO}}_{pk}(m)$
$r \xleftarrow{R} \{0,1\}^{k_0}$; $s \leftarrow (m||0^{k_1}) \oplus G(r)$
$t \leftarrow r \oplus H(s)$
$c \leftarrow (s||t)^e \bmod N$; **return** c

Algorithm $\mathcal{D}^{\mathsf{RO}}_{sk}(c)$
$s \leftarrow [c^d \bmod N]^{n+k_1}$; $t \leftarrow [c^d \bmod N]_{k_0}$
$r \leftarrow t \oplus H(s)$
$m \leftarrow [s \oplus G(r)]^n$; $p \leftarrow [s \oplus G(r)]_{k_1}$
if $(p = 0^{k_1})$ $z \leftarrow m$ **else** $z \leftarrow \perp$
return z

5.2 Universal Anonymizability of RSA-OAEP

To anonymize ciphertexts of RSA-OAEP, we do not have to employ the encoding function and we only use the expanding technique.

Definition 11. *Our universally anonymizable RSA-OAEP scheme* $\mathcal{UAPE}^{\mathsf{RO}} = ((\mathcal{K}^{\mathsf{RO}}, \mathcal{E}^{\mathsf{RO}}, \mathcal{D}^{\mathsf{RO}}), \mathcal{UA}^{\mathsf{RO}}, \mathcal{DA}^{\mathsf{RO}})$ *consists of RSA-OAEP* $\mathcal{PE}^{\mathsf{RO}} = (\mathcal{K}^{\mathsf{RO}}, \mathcal{E}^{\mathsf{RO}}, \mathcal{D}^{\mathsf{RO}})$ *and two algorithms described as follows.*

Algorithm $\mathcal{UA}^{\mathsf{RO}}_{pk}(c)$
$\alpha \xleftarrow{R} \mathrm{M}_q^{k+160}(c)$; $c' \leftarrow c + \alpha N$; **return** c'

Algorithm $\mathcal{DA}^{\mathsf{RO}}_{sk}(c')$
$c \leftarrow c' \bmod N$; $z \leftarrow \mathcal{D}^{\mathsf{RO}}_{sk}(c)$; **return** z

Our universally anonymizable RSA-OAEP scheme is CCA-secure in the random oracle model assuming RSA is one-way. (The proof is available in the full version [10].)

References

[1] Bellare, M., Boldyreva, A., Desai, A., and Pointcheval, D. Key-Privacy in Public-Key Encryption. In [3], pp. 566–582. Full version of this paper, available via `http://www-cse.ucsd.edu/users/mihir/`.

[2] Bellare, M., and Rogaway, P. Optimal Asymmetric Encryption – How to Encrypt with RSA. In *EUROCRYPT '94*, vol. 950 of *LNCS*, pp. 92–111.

[3] Boyd, C., Ed. *ASIACRYPT 2001*, vol. 2248 of *LNCS*.

[4] Cramer, R., and Shoup, V. A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack. In *CRYPTO '98*, vol. 1462 of *LNCS*, pp. 13–25.

[5] Desmedt, Y. Securing traceability of ciphertexts: Towards a secure software escrow scheme. In *EUROCRYPT '95*, vol. 921 of *LNCS*, pp. 147–157.

[6] Fujisaki, E., Okamoto, T., Pointcheval, D., and Stern, J. RSA-OAEP is Secure under the RSA Assumption. In *CRYPTO 2001*, vol. 2139 of *LNCS*, pp. 260–274.

[7] Galbraith, S. D., and Mao, W. Invisibility and Anonymity of Undeniable and Confirmer Signatures. In *CT-RSA 2003*, vol. 2612 of *LNCS*, pp. 80–97.

[8] Hayashi, R., Okamoto, T., and Tanaka, K. An RSA Family of Trap-door Permutations with a Common Domain and its Applications. In *PKC 2004* , vol. 2947 of *LNCS*, pp. 291–304.

[9] Hayashi, R., and Tanaka, K. The Sampling Twice Technique for the RSA-based Cryptosystems with Anonymity. In *PKC 2005* . vol. 3386 of *LNCS*, pp. 216–233.

[10] Hayashi, R., and Tanaka, K. Universally Anonymizable Public-Key Encryption. In *ASIACRYPT 2005*, vol. 3788 of *LNCS*, pp. 293–312.

[11] Rivest, R. L., Shamir, A., and Tauman, Y. How to Leak a Secret. In [3], pp. 552–565.